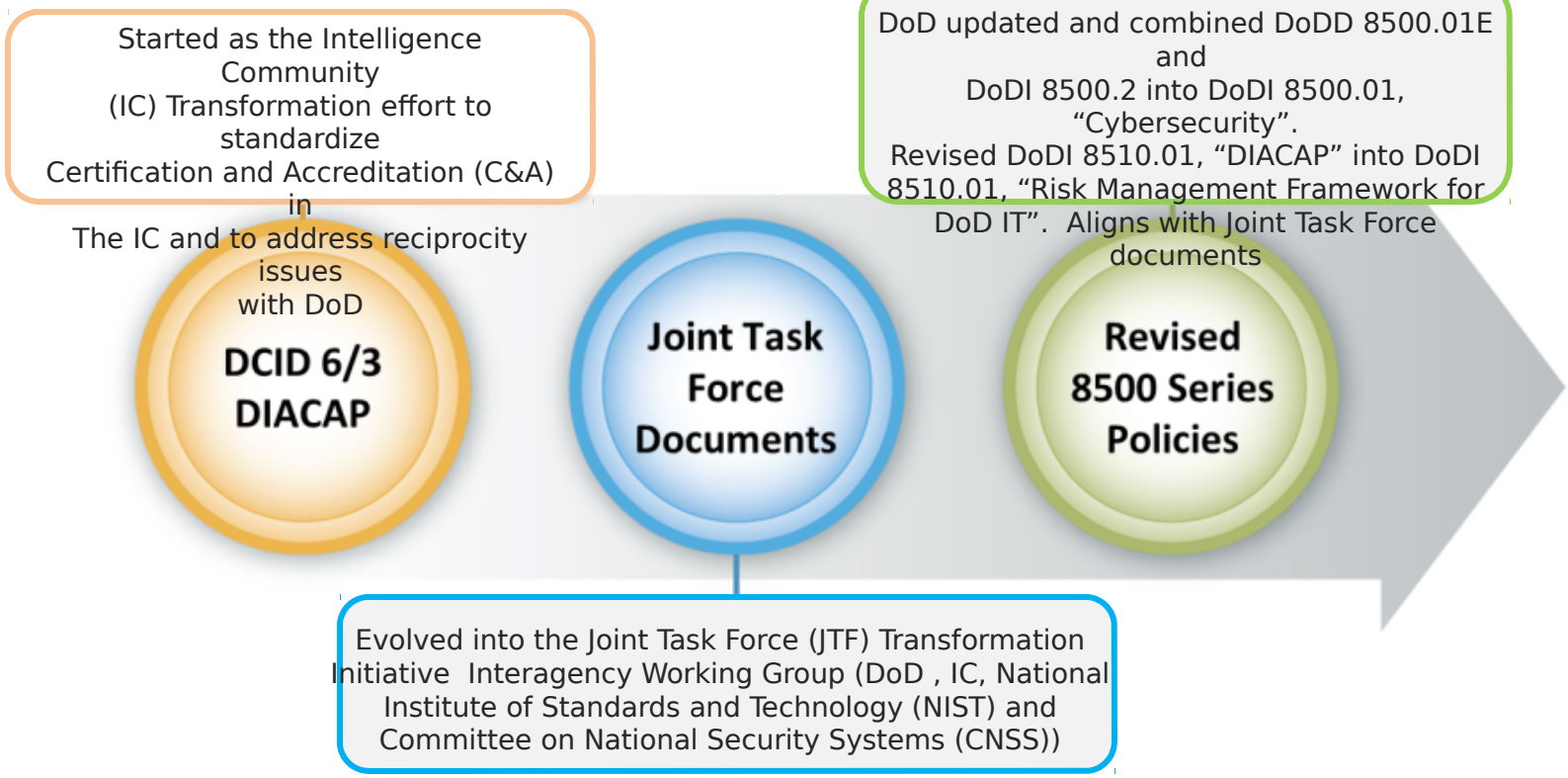
RMF

Risk Management Framework Implementation

Content Objective

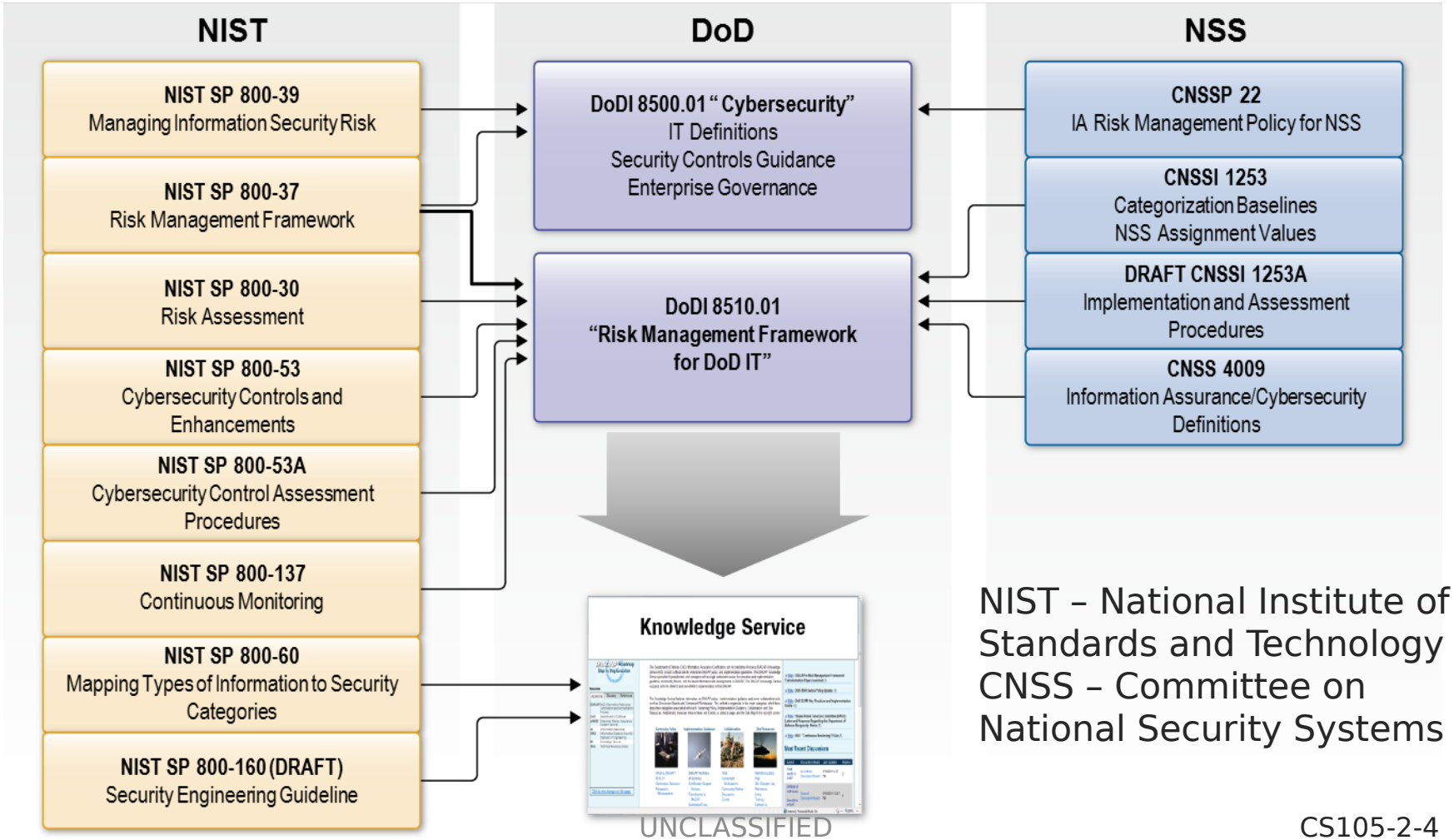
- **Introduction**
- RMF Governance
- DoD Information Technology
- RMF Knowledge Service
- Implementation Guidance
- RMF and DoD IT Acquisition
- RMF Transition Timelines

Transformation of Cybersecurity to RMF


Started as the Intelligence Community (IC) Transformation effort to standardize Certification and Accreditation (C&A) in The IC and to address reciprocity issues with DoD
DCID 6/3 DIACAP
Joint Task Force Documents
DoD updated and combined DoDD 8500.01E and DoDI 8500.2 into DoDI 8500.01, "Cybersecurity". Revised DoDI 8510.01, "DIACAP" into DoDI 8510.01, "Risk Management Framework for DoD IT". Aligns with Joint Task Force documents
Revised 8500 Series Policies
Evolved into the Joint Task Force (JTF) Transformation Initiative Interagency Working Group (DoD , IC, National Institute of Standards and Technology (NIST) and Committee on National Security Systems (CNSS))

Transformation Bottom Line – DoD will continue to follow the DoD 8500 series documentatio For Cybersecurity policy (formerly Information Assurance)

RMF Guidance Alignment



NIST – National Institute of Standards and Technology
CNSS – Committee on National Security Systems

Transition from DIACAP to the DoD RMF

The DoD RMF supports the transition from DIACAP approach to an enterprise-wide decision structure for cybersecurity risk management

Mission Assurance Category (MAC) / Confidentiality Level (CL)	**Security Objective**: Confidentiality, Integrity, Availability **Impact Value**: Low – Moderate – High
DoD Specific IA Definitions	CNSSI 4009 glossary for cybersecurity terms
DoD Security Controls	NIST SP 800-53 security control catalog. Uses CNSSI 1253 to categorize and select controls
C&A Process	Risk Management Framework Lifecycle

The Evolution of Cybersecurity and Risk

DoD Instruction (DoDI) 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT)”

- Establishes the associated cybersecurity policy and assigns responsibilities for executing and maintaining the DoD RMF
- Replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and manages the life-cycle cybersecurity risk to DoD IT
- Implements to the RMF Technical Advisory Group (TAG)
- Directs visibility of authorization documentation and artifact reuse between and among DoD Components deploying and receiving DoD IT
- Provides guidance for reciprocity of authorization decisions and artifacts within DoD, and between DoD and other federal agencies, for the authorization and connection of information systems (ISs)

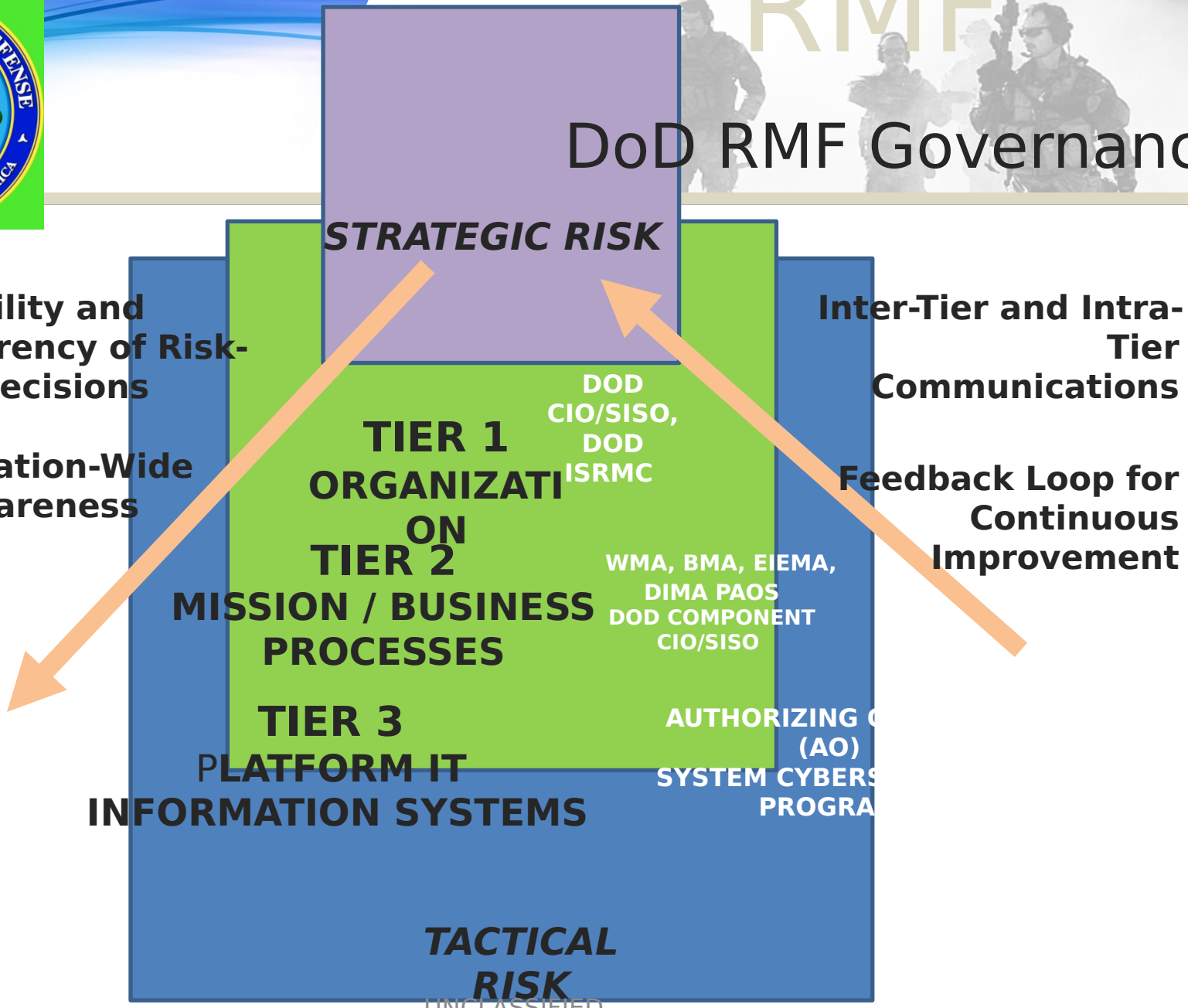
Content Objective

Governance Applicability

The DoDI 8510.01 (RMF) applies to:

- All DoD Components, except those under the authorities and policies of the Director of National Intelligence regarding the protection of sensitive compartmented information (SCI)
- All DoD-owned IT or DoD-controlled IT that receives, processes, stores, displays, or transmits DoD information, including IT that supports research, development, test and evaluation (T&E), and DoD-controlled IT operated by a contractor or other entity on behalf of the DoD

DoD RMF Governance



Tier 1 RMF Governance Structure

Tier 1 is the Office of Secretary of the Defense (OSD) and/or strategic level, and it addresses risk management at the DoD enterprise level.

The key governance elements in Tier 1 are:

- DoD CIO Directs and oversees the cybersecurity risk management of DoD IT
- Risk Executive Function DoD Information Security Risk Management Committee (ISRMC) (formerly the Defense Information Systems Network (DISN)/Global Information Grid (GIG) Flag Panel) performs the DoD Risk Executive Function. Defense IA Security Accreditation Working Group (DSAWG) supports the DoD ISRMC and develops and provides guidance to the Authorizing Officials for IS connections to the DoD Information Enterprise
- DoD Senior Information Security Officer (SISO) The DoD SISO represents the DoD CIO, directs and coordinates the DoD Cybersecurity Program, and establishes and maintains the DoD RMF
- The RMF Technical Advisory Group (TAG) The TAG provides implementation guidance for the DoD RMF
- The RMF Knowledge Service (KS) The KS is the **authoritative source** for RMF procedures and guidance. The KS supports RMF by providing access to DoD security control baselines, security control descriptions, security control overlays, and DoD implementation guidance and assessment procedures

Tier 2 RMF Governance Structure

Tier 2 are the Mission Area and Component level, and addresses risk management at this level. The key governance elements in Tier 2 are:

- Principal Authorizing Official (PAO) A PAO is appointed for each of the 4 DoD Mission Areas (MAs), the Enterprise Information Environment MA (EIEMA), Business MA (BMA), Warfighting MA (WMA), and DoD portion of the Intelligence MA (DIMA)_
- DoD Component CIO Component CIOs are responsible for administration of the RMF within the DoD Component Cybersecurity Program, including:
  - Enforcing training requirements for persons participating in the RMF
  - Verify that a Component Program Manager or System Manager is identified for each IS or Platform IT system
  - Appoint Component SISO
- Component SISO Component SISOs have authority and responsibility for security controls assessment, including:
  - Establishing and managing a coordinated security assessment process
  - Performing as the Security Controls Assessor (SCA) or formally delegate the security control assessment role

Tier 3 RMF Governance Structure

Tier 3 - is the System Level, and addresses risk management at this level. The key governance elements in **Tier 3 are:**

- **Authorizing Official (AO)** The DoD Component heads are responsible appointing trained and qualified AOs for all DoD ISs and PIT systems within their Component. AOs should be appointed from senior leadership positions within business owner and mission owner organizations
- System Cybersecurity Program The system cybersecurity program consists of the policies, procedures, and activities of the:
  - Information System Owner (ISO) Appoints a User Representative (UR) for assigned IS or PIT system
  - Program Manager/System Manager (PM/SM) Ensures an IS Systems Engineer is assigned for IS or PIT systems and implements the RMF for assigned IS or PIT systems
- User Representative (UR)
- IS Security Manager (ISSM)
- IS Security Officers (ISSO)

Content Objective

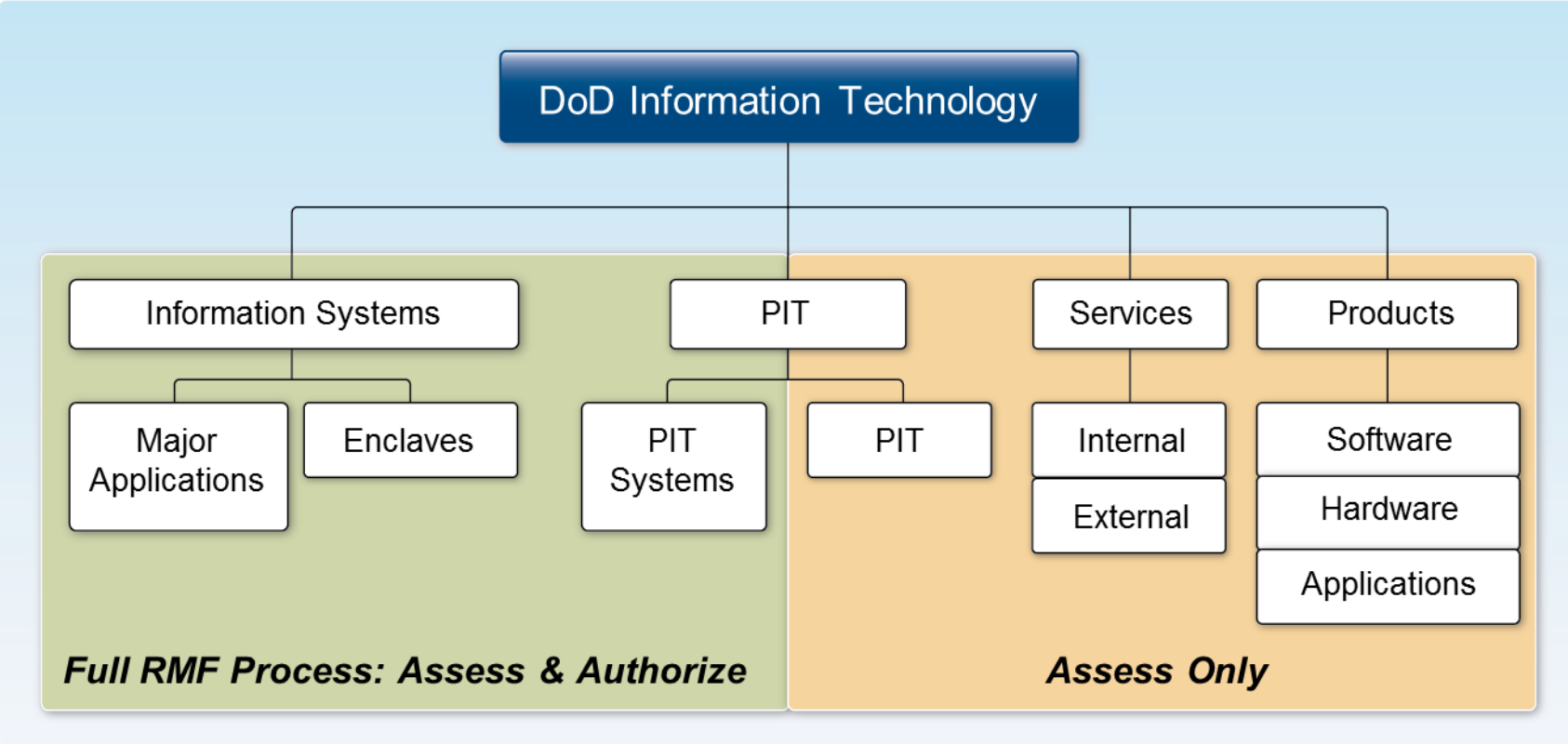
RMF Applicability

All DoD-owned IT or DoD-controlled IT that receives, process, store, displays, or transmits DoD information, including:

- All DoD information in electronic format
- Special Access Program (SAP) information technology, other than SAP ISs handling sensitive compartmented information (SCI)
- IT supporting research, development, test and evaluation (T&E), and DoD-controlled IT operated by a contractor or other entity on behalf of the DoD

DoD information technology (IT) is broadly grouped as DoD information systems (IS), platform information technology (PIT) systems, IT services, products, and PIT

DoD Information Technology Defined



Not a one size fits all approach to securing IT

Products, Services and PIT

Products, Services, and Platform IT (PIT) do not undergo the full RMF process

- Must be securely configured in accordance with applicable DoD policies and security controls
- Undergo special assessment of their functional and security-related capabilities and deficiencies
- ISSM, with concurrence of AO, is responsible for ensuring products, services, and PIT complete appropriate evaluation and configuration processes prior to incorporation into or connecting to an IS or PIT system
- RMF Knowledge Service (KS) contains additional guidance on products, services, and PIT review and assessments

Products Definition and Assessments

Products Individual IT hardware or software items (including applications) that are commercial or government provided; include but are not limited to operating systems, office productivity software, firewalls, and routers

- Will be configured in accordance with applicable Security Technical Implementation Guides (STIGs), any associated control correlation identifiers (CCIs), or Security Requirements Guides, (SRGs), as applicable, by an ISSM and security control assessor (SCA)
- STIG, CCI, and SRG compliance results will be documented as security control assessment results within a product-level security assessment report (SAR) and reviewed by the responsible ISSM (under the direction of the AO) prior being accepted into or connected to an authorized IS or PIT system

Services Definition and Assessments

IT Services IT services are outside the user organization's authorization boundary, and the user's organization has no direct control over the application or assessment of required security controls

- Internal IT Users of DoD service providers must ensure the categorization of the IS delivering the service meets the needs of the DoD organization's information and mission. Written agreements must be place that describe the roles and responsibilities of both the provider and the recipient
- External IT
  - Non-DoD federal government agency service providers must ensure the categorization of the IS delivering the service meets the needs of the DoD organization's information and mission and the IS is currently operating under an agency authorization. Interagency agreements or government statements of work must contain requirements for service level agreements (SLAs) that include application of appropriate security controls
  - Commercial or other non-federal government IT service providers must ensure the security protections of the IS delivering the service is appropriate to meet the needs of the DoD organization's information and mission. Using DoD organizations must perform categorization and appropriately tailor to determine the set of security controls to be included in requests for proposals and assess and accept the adequacy of security proposed by offerors, negotiate changes to meet DoD needs, or reject the offer. The accepted security approach must be documented in the resulting contract or order
  - Commercial cloud external IT services must comply with DoD cloud computing policy

PIT Definition and Assessments

PIT Platform IT that does not rise to the level of a PIT System may be categorized using CNSSI 1253 with the security control baselines tailored as needed. Otherwise, the specific cybersecurity needs of PIT must be assessed on a case by case basis and security controls applied as appropriate

Some e**xamples of PIT are:**

- Weapons systems, training simulators, diagnostic test and maintenance equipment
- Medical devices and health information technologies
- Vehicles and alternative fueled vehicles (e.g., electric, bio-fuel, Liquid Natural Gas that contain car-computers)
- Buildings and their associated control systems
- Utility distribution systems
  - Electric, water, waste water, natural gas and steam
- Telecommunications systems designed specifically for industrial control systems
  - Supervisory control and data acquisition (SCADA), direct digital control, programmable logic controllers, other control devices and advanced metering

RMF Facilitates Reciprocity

Applied appropriately, reciprocity reduces redundant testing, assessing and documentation, and the associated costs in time and resources

The DoD RMF presumes acceptance of existing test and assessment results and authorization documentation

DoDI 8510, Enclosure 5, provides use cases describing the proper application of DoD policy on reciprocity in the most frequently occurring scenarios

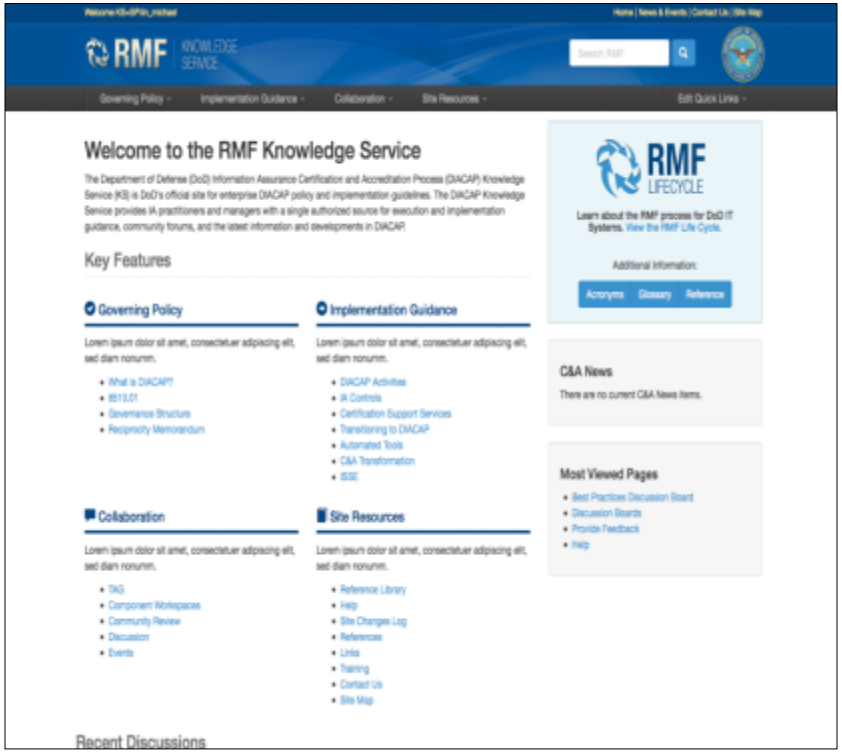
Reciprocity Approach for System Acceptance

1. Review the complete security authorization package
2. Determine the security impact of connecting the deploying system within the receiving enclave or site
3. Determine the risk of hosting the deploying system within the enclave or site
4. If the risk is acceptable, execute a documented agreement between deploying and receiving organizations
5. Document the acceptance by the receiving AO
6. Update the receiving enclave or site authorization documentation for inclusion of the deployed system

Content Objective

RMF Knowledge Service

The Knowledge Service is the **authoritative source** for information, guidance, procedures, and templates on how to execute the Risk Management Framework



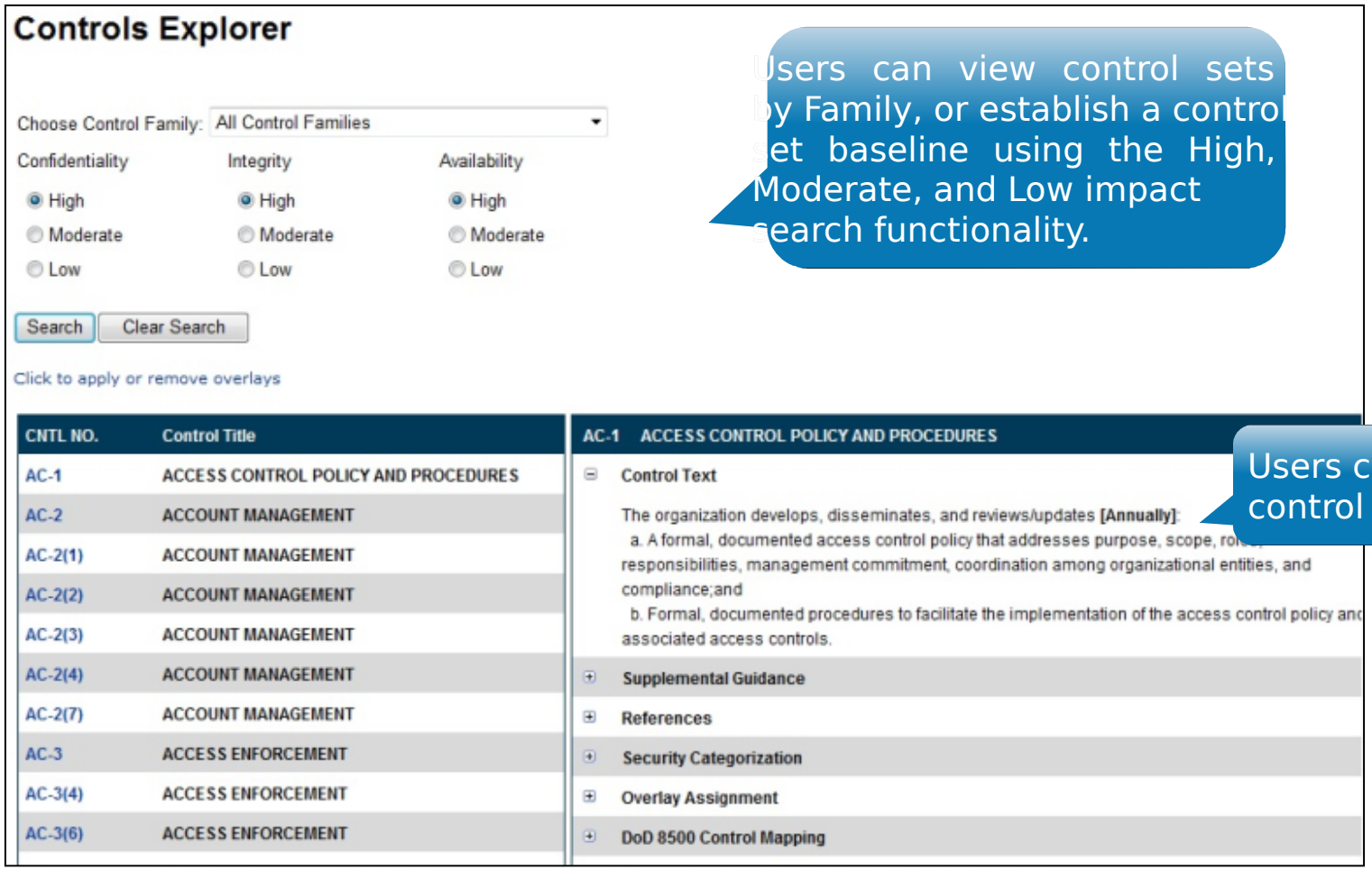
URL for RMF KS: https://rmfks.osd.mil

RMF Knowledge Service Overview

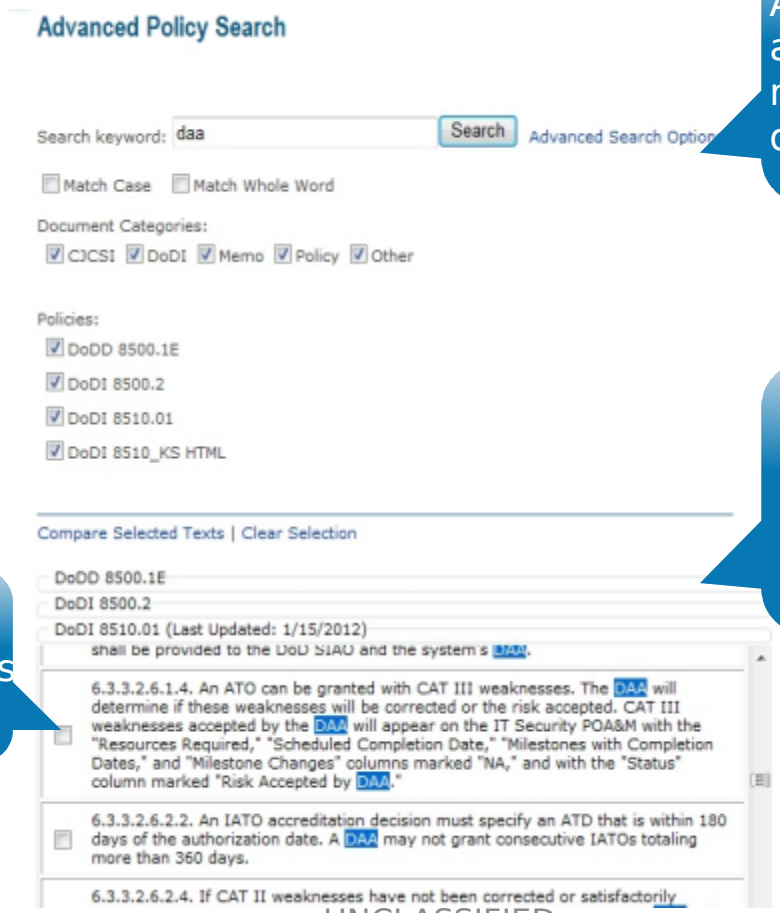
Knowledge Service

- A web-based, DoD Public Key Infrastructure (PKI)-enabled resource
- Developed under the ownership and authority of DoD CIO
- An information repository and collaboration forum for the RMF Technical Advisory Group (TAG) and corresponding TAG Working Groups
- A collaboration workspace for the RMF user community to develop, share and post lessons learned and best practices
- A library of tools, diagrams, process maps, documents, etc., to support and aid in execution of the RMF
- A source for cybersecurity news and events and other cybersecurity-related information resources
- Serves and supports the DIACAP as well as the RMF

Supports NIST SP 800-53 and CNSSI 1253



KS Advanced Policy Search Capability


Advanced Policy Search
Search keyword: daa
Search
Advanced Search Option
Match Case
Match Whole Word
Document Categories:
CJCSI
DoDI
Memo
Policy
Other
Policies:
DoDD 8500.1E
DoDI 8500.2
DoDI 8510.01
DoDI 8510_KS HTML
Compare Selected Texts | Clear Selection
DoDD 8500.1E
DoDI 8500.2
DoDI 8510.01 (Last Updated: 1/15/2012)
shall be provided to the DoD SIAO and the system's DAA.
6.3.3.2.6.1.4. An ATO can be granted with CAT III weaknesses. The DAA will determine if these weaknesses will be corrected or the risk accepted. CAT III weaknesses accepted by the DAA will appear on the IT Security POA&M with the "Resources Required," "Scheduled Completion Date," "Milestones with Completion Dates," and "Milestone Changes" columns marked "NA," and with the "Status" column marked "Risk Accepted by DAA."
6.3.3.2.6.2.2. An IATO accreditation decision must specify an ATD that is within 180 days of the authorization date. A DAA may not grant consecutive IATOs totaling more than 360 days.
6.3.3.2.6.2.4. If CAT II weaknesses have not been corrected or satisfactorily

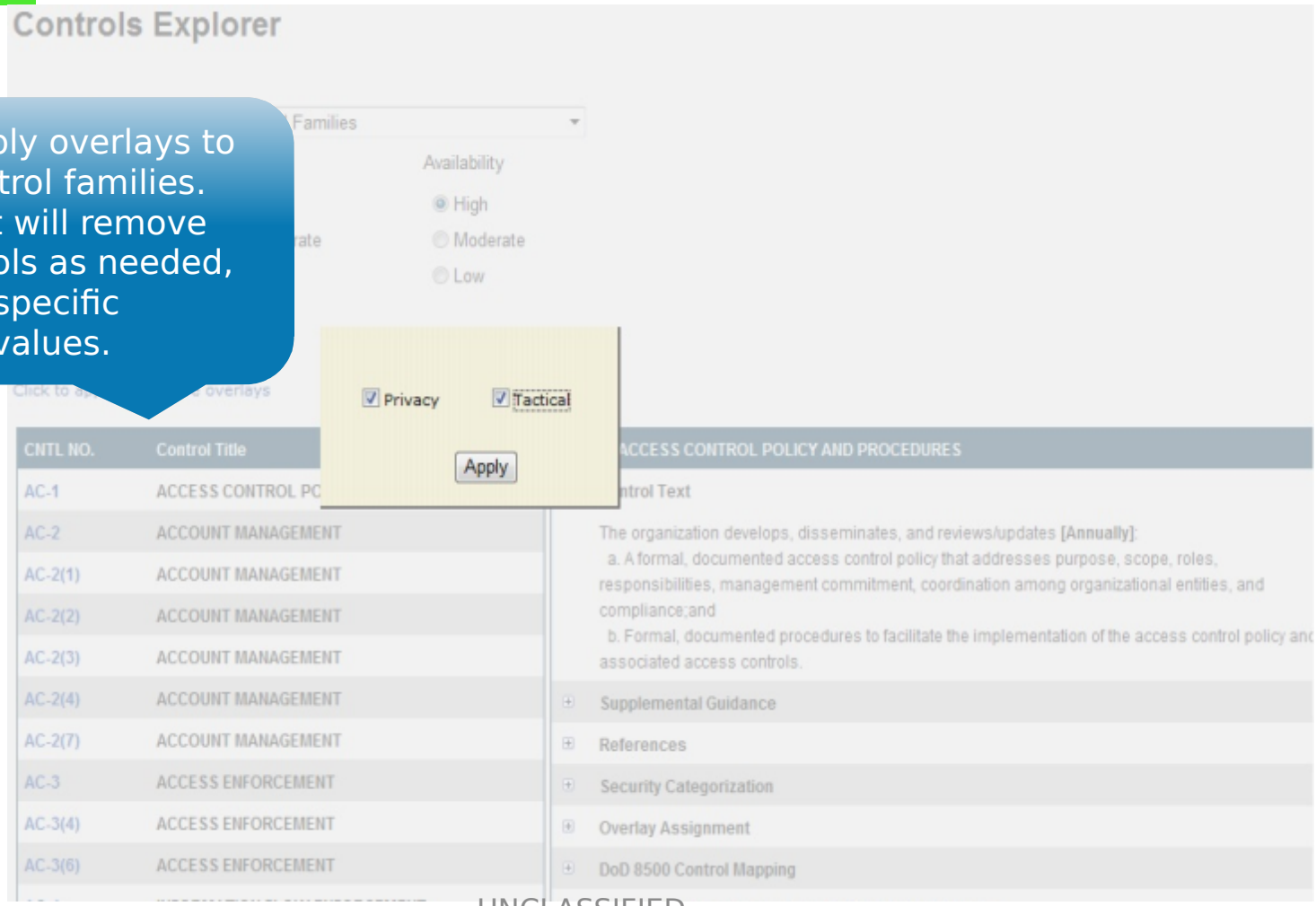
Advanced search options allow users to search across multiple policies, and select document categories.

Results are displayed by Policy, by paragraph, in an accordion format with the keyword search highlighted.

Users have the ability to compare paragraphs across policies.

KS Instructs on Applying Overlays

Ability to apply overlays to baseline control families. Resulting set will remove or add controls as needed, and change specific assignment values.



Applying Overlays Continued

CNTL NO.	Control Title
AC-1	ACCESS CONTROL POLICY AND PROCEDURES
AC-2	ACCOUNT MANAGEMENT
AC-2(1)	ACCOUNT MANAGEMENT
AC-2(2)	ACCOUNT MANAGEMENT
AC-2(3)	ACCOUNT MANAGEMENT
AC-2(4)	ACCOUNT MANAGEMENT
AC-2(7)	ACCOUNT MANAGEMENT
AC-3	ACCESS ENFORCEMENT
AC-3(4)	ACCESS ENFORCEMENT
AC-3(6)	ACCESS ENFORCEMENT
AC-4	INFORMATION FLOW ENFORCEMENT
AC-4(12)	INFORMATION FLOW ENFORCEMENT
AC-4(15)	INFORMATION FLOW ENFORCEMENT
AC-5	SEPARATION OF DUTIES
AC-6	LEAST PRIVILEGE
AC-6(1)	LEAST PRIVILEGE
AC-6(2)	LEAST PRIVILEGE
AC-6(3)	LEAST PRIVILEGE
AC-6(4)	LEAST PRIVILEGE
AC-6(5)	LEAST PRIVILEGE

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control Text

The organization develops, disseminates, and reviews/updates **[Annually]**:
a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;and
b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Supplemental Guidance

This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the access control family. The policy and procedures are cor
policies, regulations, standards, a
Existing organizational policies ar
and procedures unnecessary.
The access control policy can be
organization.
Access control procedures can be
information system, when require
The organizational risk managemen
policy.

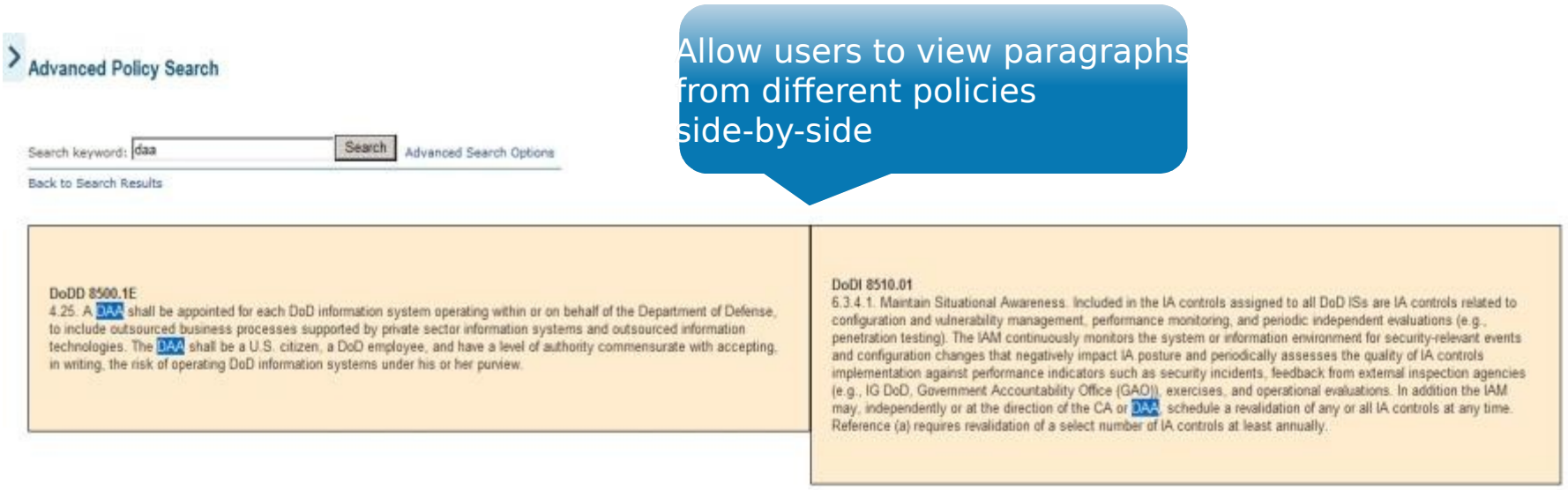
Privacy Overlay: PHI Subset: If the organization is a covered entity the organization develops, disseminates, and reviews/updates the access control policies and procedures satisfying the HIPA Minimum Necessary Rule as stated in 45 CFR 164.514(d)(1) – (5) to limit unnecessary or inappropriate access to protected health information. The organization establishes procedures for privileged accounts that may have access to PHI. (See Definitions for covered entity and Minimum Necessary Rule.)

Related Controls
undefined

Applied overlays displayed in the Supplemental Guidance Section of controls details

KS Compares Policy Documents

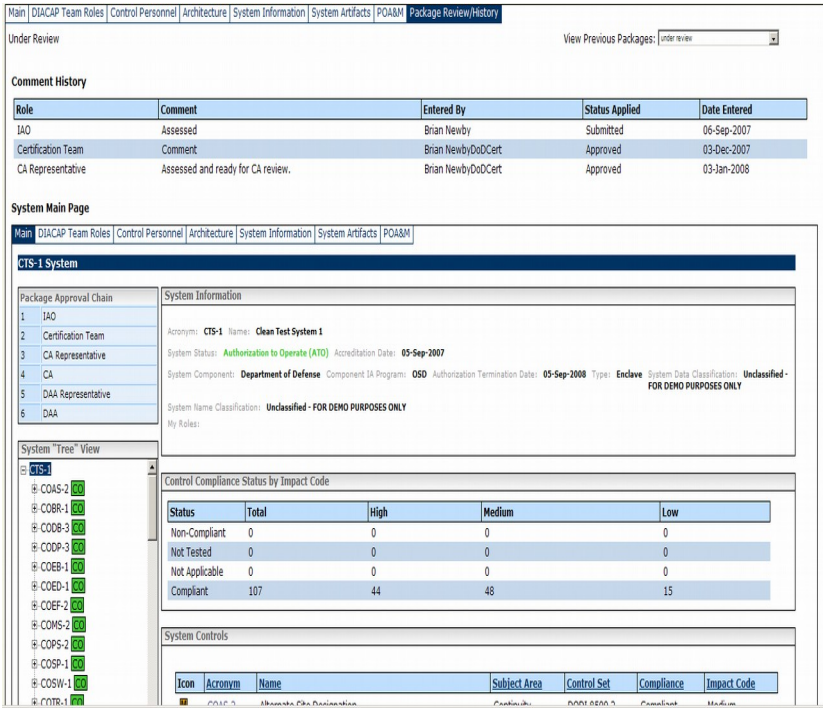
Compare Paragraphs from Different Policies


Advanced Policy Search
Search keyword: daa
Search
Advanced Search Options
Back to Search Results
Allow users to view paragraphs from different policies side-by-side
DoDD 8500.1E
4.25. A DAA shall be appointed for each DoD information system operating within or on behalf of the Department of Defense, to include outsourced business processes supported by private sector information systems and outsourced information technologies. The DAA shall be a U.S. citizen, a DoD employee, and have a level of authority commensurate with accepting, in writing, the risk of operating DoD information systems under his or her purview.
DoDI 8510.01
6.3.4.1. Maintain Situational Awareness. Included in the IA controls assigned to all DoD ISs are IA controls related to configuration and vulnerability management, performance monitoring, and periodic independent evaluations (e.g., penetration testing). The IAM continuously monitors the system or information environment for security-relevant events and configuration changes that negatively impact IA posture and periodically assesses the quality of IA controls implementation against performance indicators such as security incidents, feedback from external inspection agencies (e.g., IG DoD, Government Accountability Office (GAO)), exercises, and operational evaluations. In addition the IAM may, independently or at the direction of the CA or DAA, schedule a revalidation of any or all IA controls at any time. Reference (a) requires revalidation of a select number of IA controls at least annually.

RMF Encourages Use of Automated Tools

Some Security Controls, baselines, Security Requirements Guides (SRGs), Security Technical Implementation Guides (STIGs), Control Correlation Identifiers (CCIs), implementation and assessment procedures, overlays, common controls, etc., *may possibly* be automated

- Automated systems are being developed to manage the RMF workflow process, to identify key decision points, and to generate control lists needed in RMF implementation
- An example of such an automated system is the DoD-sponsored Enterprise Mission Assurance Support Service (eMASS)


Main | DIACAP Team Roles | Control Personnel | Architecture | System Information | System Artifacts | POA&M | Package Review/History
Under Review
View Previous Packages:
Comment History
Role | Comment | Entered By | Status Applied | Date Entered
IAO | Assessed | Brian Newby | Submitted | 06-Sep-2007
Certification Team | Comment | Brian NewbyDoDCert | Approved | 03-Dec-2007
CA Representative | Assessed and ready for CA review. | Brian NewbyDoDCert | Approved | 03-Jan-2008
System Main Page
Main | DIACAP Team Roles | Control Personnel | Architecture | System Information | System Artifacts | POA&M
CTS-1 System
Package Approval Chain
1 IAO
2 Certification Team
3 CA Representative
4 CA
5 DAA Representative
6 DAA
System Information
Acronym: CTS-1 Name: Clean Test System 1
System Status: Authorization to Operate (ATO) Accreditation Date: 05-Sep-2007
System Component: Department of Defense Component IA Program: OSD Authorization Termination Date: 05-Sep-2008 Type: Enclave System Data Classification: Unclassified - FOR DEMO PURPOSES ONLY
System Name Classification: Unclassified - FOR DEMO PURPOSES ONLY
My Roles:
System "Tree" View
CTS-1
COAS-2 CO
COBR-1 CO
CODB-3 CO
CODP-3 CO
COEB-1 CO
COED-1 CO
COEF-2 CO
COMS-2 CO
COPS-2 CO
COSP-1 CO
COSW-1 CO
Control Compliance Status by Impact Code
Status | Total | High | Medium | Low
Non-Compliant | 0 | 0 | 0 | 0
Not Tested | 0 | 0 | 0 | 0
Not Applicable | 0 | 0 | 0 | 0
Compliant | 107 | 44 | 48 | 15
System Controls
Icon | Acronym | Name | Subject Area | Control Set | Compliance | Impact Code

Content Objective

RMF Step 1

Step 1 CATEGORIZE System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2 SELECT Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve Security Plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3 IMPLEMENT Security Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in Security Plan

Step 4 ASSESS Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5 AUTHORIZE System

- **Prepare the POA&M**
- **Submit Security Authorization Package (Security Plan, SAR, and POA&M) to AO**
- **AO conducts final risk determination**
- **AO makes authorization decision**

Step 6 MONITOR Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update Security Plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

Step 1 – Categorize System

Categorize System(s) Not all DoD ISs are National Security Systems (NSS); however, the same standards and process for categorizing NSS apply to non-NSS

- Categorize the system IAW CNSSI 1253 and document results in the Security Plan
- Describe the system (include system boundaries) and document description in the Security Plan
- Register the system in the DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles and document team member assignments in the Security Plan

CNSSI 1253 System Categorization

The CNSSI 1253 System Categorization process is required by DoD 8510.01 for all information systems and PIT systems for both NSS and non-NSS

- Builds on and is a companion document to NIST Special Publication SP 800-53
- Should be used as a tool by ISSEs, AOs, SISOs, ISSOs, Data Owners and others to select and agree upon appropriate protections for an IS or PIT system
- Based upon FIPS 199, Categorize NSS using three security objectives (confidentiality, integrity, and availability) with one impact value (low, moderate, or high) for each of the security objectives
- Defines and provides guidance on developing and implementing overlays

CNSSI Security Control Baseline

Table D-1: NSS Security Control Baselines

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X
AC-2	Account Management	X	X	X	X	X	X			
AC-2(1)	Account Management | Automated System Account Management		X	X		X	X			
AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts		X	X		X	X			
AC-2(3)	Account Management | Disable Inactive Accounts		X	X		X	X			
AC-2(4)	Account Management | Automated Audit Actions	+	X	X	+	X	X			
AC-2(5)	Account Management | Inactivity Logout							+	+	X
AC-2(6)	Account Management | Dynamic Privilege Management									
AC-2(7)	Account Management | Role-Based Schemes	+	+	+	+	+	+			
AC-2(8)	Account Management | Dynamic Account Creation									
AC-2(9)	Account Management | Restrictions on Use of Shared Groups / Accounts	+	+	+	+	+	+			
AC-2(10)	Account Management | Shared / Group Account Credential Termination	+	+	+	+	+	+			
AC-2(11)	Account Management | Usage Conditions									
AC-2(12)	Account Management | Account Monitoring / Atypical Usage	+	+	X	+	+	X			
AC-2(13)	Account Management | Disable Accounts For High-Risk Individuals	+	+	X	+	+	X			
AC-3	Access Enforcement	X	X	X	X	X	X			

"X" = Security Controls from NIST Baselines

"+" = Security Controls Added for Protection of NSS

Not all DoD ISs are NSS, however, the same standards and processes under the RMF also apply to ISs that are not NSSs

Example of a CNSSI 1253 Security Control Baseline for a NSS

RMF Step 2

Step 1 CATEGORIZE System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2 SELECT Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve Security Plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3 IMPLEMENT Security Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in Security Plan

Step 4 ASSESS Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5 AUTHORIZE System

- **Prepare the POA&M**
- **Submit Security Authorization Package (Security Plan, SAR, and POA&M) to AO**
- **AO conducts final risk determination**
- **AO makes authorization decision**

Step 6 MONITOR Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update Security Plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

RMF

Step 2 – Select Security Controls

Security Control Selection

- Identify Common Controls
- Identify Security Control Baseline and select any applicable overlays
- Tailor baseline controls as necessary
- Supplement the tailored baseline security control set, if necessary
- Document resulting security controls, supporting selection rationale, and system use limitation in the security plan
- Develop and document a system level strategy for the continuous monitoring of the effectiveness of the employed security controls
- Authorizing Official reviews and approves the security plan and the system-level continuous monitoring strategy

Security Control Catalog (NST SP 800-53)

Security Controls Address Current Threats

- Advanced Persistent Threat
- Insider Threat (incl. Removable Media)
- Supply Chain
- Cross Domain
- Identity Management

AC-1 Access Control Policy and Procedure

AC-2 Account Management

AT-1 Security Awareness and Training Policy and Procedures

AT-2 Security Awareness

AU-1 Audit and Accountability Policy and Procedures

AU-2 Auditable Events

CA-1 Security Assessment and Authorization Policy and Procedures

CM-1 Configuration Management Policy and Procedures

Enterprise-wide Authorization ISs & Services

Common Control

- Security control that is inherited by one or more organizational information systems

Security Control Inheritance

- Information system or application receives protection from security controls (or portions of security controls) that are developed, authorized, and monitored by another organization, either internal or external, to the organization where the system or application resides

Of the 900+ controls and enhancements in the NIST SP 800-53 Rev. 4 Catalog, about 400 typically apply to an IS. Of the 400, many are "common controls" inherited from the hosting environment; this is great use of the "build once/use many" approach.

Overlays

Overlays address additional factors beyond impact (baselines only address impact of loss of confidentiality, integrity, and availability)

Enterprise Tailoring

- Consistent approach and set of security controls by subject area
- One time resource expenditure vs. continued expenditures of single system tailoring
- Promotes reciprocity

DoD Overlay Examples

Approved Overlays	Overlays in Development (VETTED)	Proposed Overlays (NOT VETTED)
• Intelligence (FOUO, October 2012) • Space Platforms (June 2013) • Cross Domain Solutions (September 2013)	• Classified Information • Privacy Information • Tactical Environment • Industrial Control Systems • Information Accessibility	**Formally Submitted to CS SWG** • Research Development Test & Evaluation • Modeling & Simulation **Informal Suggestions** • Cloud • DECC/Data Center • Nuclear Command and Control • Platform IT • Mobile/Wireless Networking • Medical Systems • CUI • PKI • DoD SAPs
Total: 3	5	11

RMF Step 3

Step 1 CATEGORIZE System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2 SELECT Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve Security Plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3 IMPLEMENT Security Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in Security Plan

Step 4 ASSESS Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5 AUTHORIZE System

- **Prepare the POA&M**
- **Submit Security Authorization Package (Security Plan, SAR, and POA&M) to AO**
- **AO conducts final risk determination**
- **AO makes authorization decision**

Step 6 MONITOR Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update Security Plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

RMF

Step 3 – Implement Security Controls

Implement Security Controls

- As specified in the Security Plan
- Products with IS or PIT system boundaries will be configured IAW STIGs, SRGs, or CCIs
- Controls will be implemented IAW DoD Component architectures and standards
- Implementation teams must be qualified IAW DoD 8570.01-M
- Document Security Control implementation IAW guidance contained in the RMF KS
- Identified common controls available for inheritance will show compliance status provided by hosting or connected systems

NOTE: These bullets are a sub-set of the main implementation activities, highlighted because they have significant importance

RMF Step 4

Step 1 CATEGORIZE System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2 SELECT Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve Security Plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3 IMPLEMENT Security Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in Security Plan

Step 4 ASSESS Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5 AUTHORIZE System

- **Prepare the POA&M**
- **Submit Security Authorization Package (Security Plan, SAR, and POA&M) to AO**
- **AO conducts final risk determination**
- **AO makes authorization decision**

Step 6 MONITOR Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update Security Plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

RMF

Step 4 – Assess Security Controls

Assess Security Controls

- Assess the security controls in accordance with the assessment procedures defined in the security assessment plan
- Develop, review, and approve a plan to assess the security controls
- Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment
- Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate

Assessment Steps

Develop the Security Assessment Plan

- The Security Control Assessor (SCA) develops the Security Assessment Plan
  - Ensures assessment activities are coordinated for interoperability, DT&E and OT&E events
  - Selects appropriate procedures to assess those controls
  - Tailors the assessment procedures
  - Finalizes the plan and obtains approval
- The AO approves the Security Assessment Plan

DoD RMF KS contains guidance on assessment procedures

- Explains integration of assessment procedures of applicable Security Technical Implementation Guides (STIGs), any associated Control Correlation Identifiers (CCIs), or Security Requirements Guides (SRGs)

Conduct the Assessment

Conduct the Assessment

- NIST SP 800-30 is the guide for conducting risk assessments
- The KS is the authoritative source for DoD security control assessment procedures
- SRG and STIG compliance results will be used as part of the overall security control assessment
- SCAs will maximize the reuse of existing assessments (i.e., a leveraged authorization)
- The SCA will determine a risk level for every non-compliant (NC) security control in the system baseline
- Vulnerability severity values will be assigned to all NC controls by the SCA

Conduct the Assessment

Conduct the Assessment (Continued)

- The results of all security control assessments in the control set will be recorded in the Security Assessment Report (SAR)
- The SCA must determine and document in the SAR an assessment of overall system level of risk
- The risk assessment must address the impact of all NC controls and clearly communicate the SCA's conclusion on system cybersecurity risk

Security Assessment Report

Create the Security Assessment Report

- The SAR documents the SCA's findings of compliance with assigned security controls based on actual assessment results
- The SAR addresses security controls in a NC status, including existing and planned mitigations
- A SAR is always required before an authorization decision
- If a compelling mission or business need requires the rapid development of a new system, assessment activity and a SAR are still required

RMF Step 5

Step 1 CATEGORIZE System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2 SELECT Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve Security Plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3 IMPLEMENT Security Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in Security Plan

Step 4 ASSESS Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5 AUTHORIZE System

- **Prepare the POA&M**
- **Submit Security Authorization Package (Security Plan, SAR, and POA&M) to AO**
- **AO conducts final risk determination**
- **AO makes authorization decision**

Step 6 MONITOR Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update Security Plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

RMF

Step 5 – Authorize System

Authorize System

- Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken
- Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation
- Assemble the security authorization package and submit the package to the authorizing official.

Finalize POA&M

Finalize POA&M

- Prepare the plan of action and milestones (POA&M) based on the vulnerabilities identified during the security control assessment
- Templates for preparing a POA&M are provided in the KS
- POA&Ms are maintained throughout the system life cycle. Once posted to the POA&M, vulnerabilities will be updated after correction or mitigation actions are completed, but not removed
- Component SISOs must monitor and track the overall execution of system-level POA&Ms across the entire Component

DoD Authorization Decisions

Authorization Decisions

- AO renders a final determination of risk to DoD operations and assets, individuals, other organizations, and the Nation from the operation and use of the system. The RMF KS provides additional guidance and tools
- An authorization decision applies to a specifically identified IS or PIT system and balances mission need against risk to the mission
- DoD authorization decision is expressed as an Authorization To Operate (ATO), an Interim Authorization to Test (IATT), or a Denial of Authorization to Operate (DATO). An IS or PIT system is considered unauthorized if an authorization decision has not been made
- Security authorization package consists of: Security Plan (SP), Security Assessment Report (SAR), POA&M, and authorization decision document (ATO, IATT, DATO)

DoD Authorization Decisions (Cont.)

Authorization Decision and Authorization Decision Documents

- If overall risk is determined to be acceptable, and there are no NC controls with a level of risk of “Very High” or “High,” then the authorization decision should be issued as an ATO
- NC controls with a level of risk of “Very High” or “High” exist that cannot be corrected or mitigated immediately, but overall system risk is determined to be acceptable due to mission criticality, then the authorization decision should be issued as an ATO with conditions and only with permission of the responsible DoD Component CIO
- NC controls with a level of risk of “Very High” or “High” must also be reported to the DoD ISRMC
- If risk is determined to be unacceptable, the authorization decision should be issued in the form of a DATO
- If the risk determination is being made to permit testing of the system in an operational information environment or with live data, and the risk is acceptable, then the authorization decision should be issued in the form of an IATT
- Operation of a system under an IATT in an operational environment is for testing purposes only (i.e., the system will not be used for operational

RMF Step 6

Step 1
CATEGORIZE System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2
SELECT Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve Security Plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3
IMPLEMENT Security Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in Security Plan

Step 4
ASSESS Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5
AUTHORIZE System

- **Prepare the POA&M**
- **Submit Security Authorization Package (Security Plan, SAR, and POA&M) to AO**
- **AO conducts final risk determination**
- **AO makes authorization decision**

Step 6
MONITOR Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update Security Plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

RMF

UNCLASSIFIED

Step 6 – Monitor Security Controls

Monitor Security Controls

- Determine the security impact of proposed or actual changes to the information system and its environment of operation
- Assess a selected subset of the technical, management, and operational security controls annually that are employed within and inherited by the information system in accordance with the organization-defined monitoring strategy
- Conduct selected remediation actions based on the results of ongoing monitoring activities, assessment of risk, and the outstanding items in the plan of action and milestones
- Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process

Step 6 -Monitor Security Controls

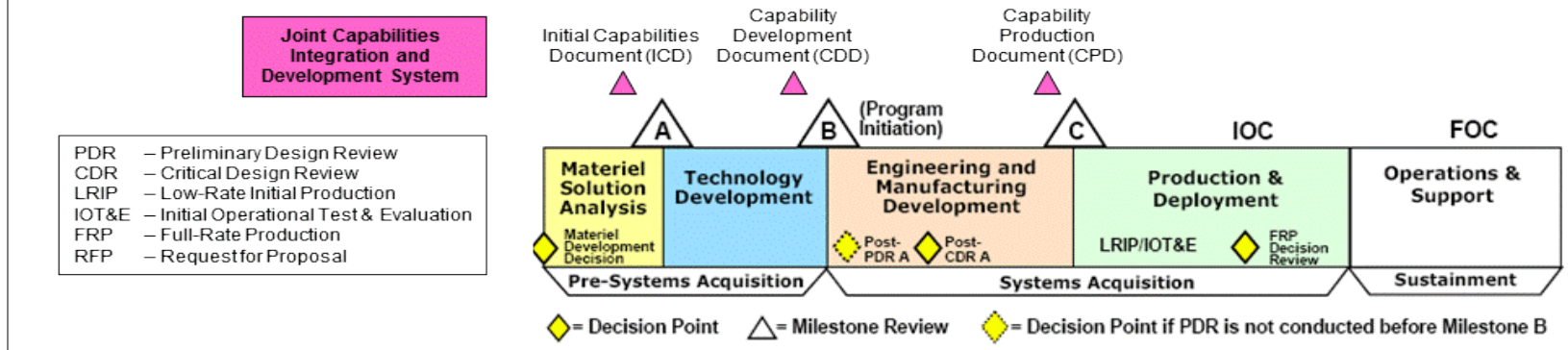
Monitor Security Controls (Continued)

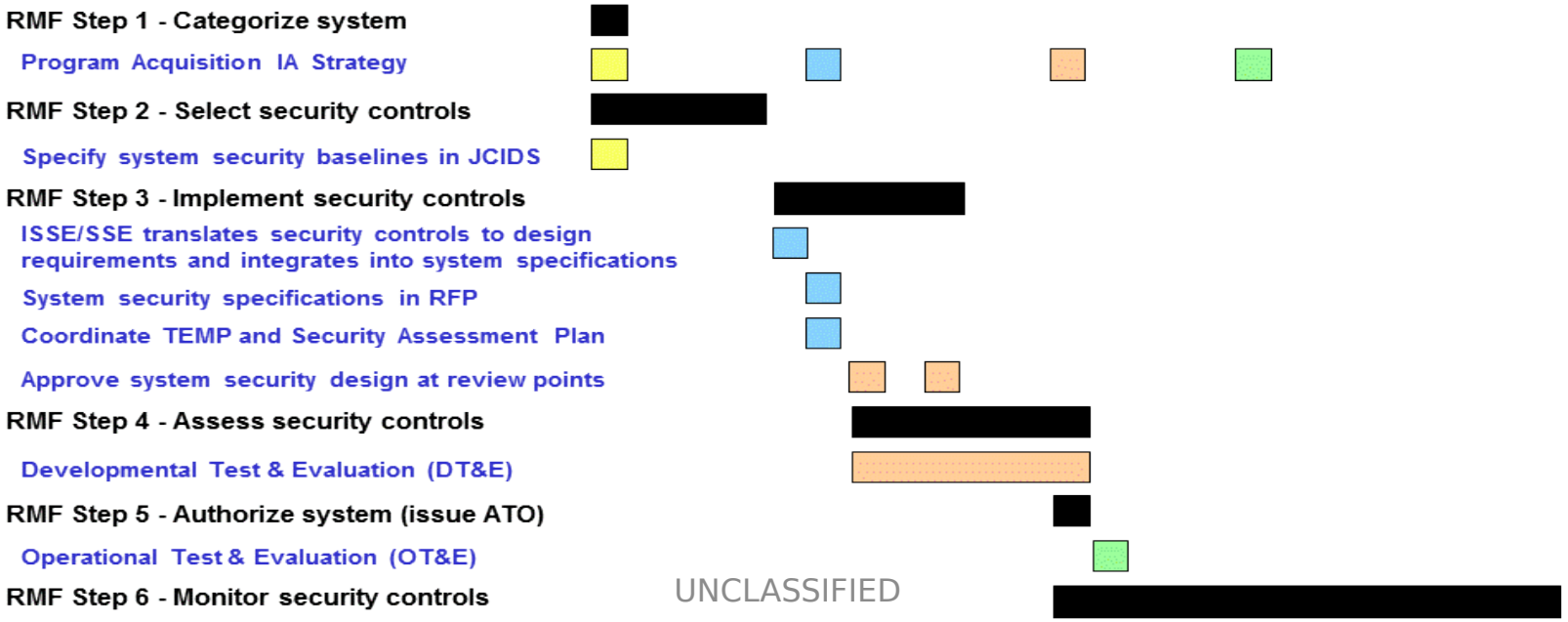
- Report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the AO on an ongoing basis in accordance with the organization-defined monitoring strategy
- AO reviews the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable
- The assessor must provide a written and signed (or if digital, DoD PKI-certified digitally signed) report in the SAR format to the AO that indicates the results of an annual assessment of selected security controls
- Implement an information system decommissioning strategy which executes required actions when a system is removed from service

Content Objective

RMF Built into DoD Acquisition Lifecycle

Alignment of RMF and DoD Acquisition System Activities




RMF Step 1 - Categorize system
Program Acquisition IA Strategy
RMF Step 2 - Select security controls
Specify system security baselines in JCIDS
RMF Step 3 - Implement security controls
ISSE/SSE translates security controls to design requirements and integrates into system specifications
System security specifications in RFP
Coordinate TEMP and Security Assessment Plan
Approve system security design at review points
RMF Step 4 - Assess security controls
Developmental Test & Evaluation (DT&E)
RMF Step 5 - Authorize system (issue ATO)
Operational Test & Evaluation (OT&E)
RMF Step 6 - Monitor security controls

UNCLASSIFIED

Content Objective

RMF Transition Timelines

System Authorization Status	Transition Timeline And Instructions
New start or unaccredited	Transition to the RMF within six months
System has initiated DIACAP but has not yet started executing the DIACAP Implementation Plan	Transition to the RMF within six months
System has begun executing the DIACAP Implementation Plan	**Either:** a. Develop a strategy and schedule for transitioning to the RMF not to exceed the system re-authorization timeline **or,** b. Transition to the RMF within six months
System has a current valid DIACAP accreditation decision	Develop a strategy and schedule for transitioning to the RMF not to exceed the system re-authorization timeline
System has a DIACAP accreditation that is more than 3 years old	Transition to the RMF within six months

Regardless of status, you should immediately begin planning to transition to the RMF

Questions